



Docket No. 43521-0700

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Hidema TANAKA et al.

Serial No.: 10/622,722

Filed: July 18, 2003

For: CIPHER STRENGTH ESTIMATING DEVICE

Examiner: TBA

Group Art Unit: TBA

January 26, 2004

Irvine, California 92614

INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In an attempt to fully comply with the duty of disclosure set forth in 37 C.F.R. § 1.56 and in conformance with 37 C.F.R. §§ 1.97 and 1.98, applicant wishes to bring to the attention of the U.S.

Patent Office the following references:

Babbage & Frisch "On MISTY1 Higher Order Differential Cryptanalysis"
Daemen, Knudsen & Rijmen "The Block Cipher SQUARE"
Jakobsen & Knudsen "The Interpolation Attack on Block Cipher"
Nyberg & Knudsen, "Provable Security Against Differential Cryptanalysis"
Shimoyama, Moriai & Kaneko, "Improving the Higher Order Differential Attack and Cryptanalysis of the KN Cipher"
Tanaka, Hisamatsu & Kaneko, "Strength of MISTY1 without FL Function for Higher Order Differential Attack"

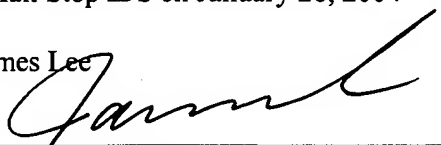
Copies of these references and a form PTO-A820 are attached.

Docket No. 43521-0700

If the Examiner believes that a telephone conference would help further the prosecution of this case, he is respectfully requested to contact the undersigned attorney at the listed telephone number.

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, Mail Stop IDS on January 26, 2004

by: James Lee

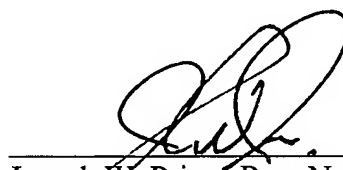


Signature

Date of Signature: January 26, 2004

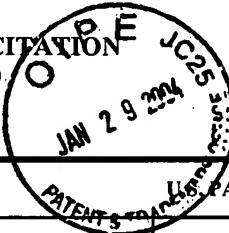
Very truly yours,

SNELL & WILMER LLP



Joseph W. Price, Reg. No. 25,124
1920 Main Street, Suite 1200
Irvine, CA 92614
949/253-4924

INFORMATION DISCLOSURE CITATION <i>(Use several sheets if necessary)</i>				Docket Number (Optional) 43521-0700		Application Number 10/622,722	
				Applicant(s) Hidema TANAKA, Toshinobu KANEKO			
				Filing Date July 18, 2003		Group Art Unit TBA	



U.S. PATENT DOCUMENTS							
*EXAMINER INITIAL	REF	DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE

FOREIGN PATENT DOCUMENTS								
	REF	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	Translation	
							YES	NO

OTHER DOCUMENTS <i>(Including Author, Title, Date, Pertinent Pages, Etc.)</i>		
		Jakobsen & Knudsen "The Interpolation Attack on Block Cipher," FSE-4th International Workshop LNCS 1008
		Nyberg, Knudsen, "Provable Security Against Differential Cryptanalysis," Journal of Cryptology, Vol. 8-no. 1

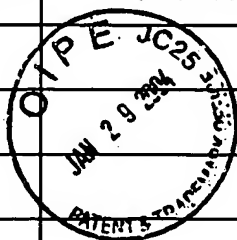
EXAMINER	DATE CONSIDERED
----------	-----------------

EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP Section 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

INFORMATION DISCLOSURE CITATION <i>(Use several sheets if necessary)</i>	Docket Number (Optional) 43521-0700	Application Number 10/622,722
	Applicant(s) Hidema TANAKA, Toshinobu KANEKO	
	Filing Date July 18, 2003	Group Art Unit TBA

U.S. PATENT DOCUMENTS

*EXAMINER INITIAL	REF	DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE



FOREIGN PATENT DOCUMENTS

	REF	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	Translation	
							YES	NO

OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, Etc.)*

		Shimoyama, Moriai, Kaneko, "Improving the Higher Order Differential Attack and Cryptanalysis of the KN Cipher," 1997 1st International Workshop on Information Security Workshop LNCS 1396, Tatsunokuchi, Ishikawa, Japan, September 1997 (pp 32-42)
		Tanaka, Hisamatsu, Kaneko, "Strength of MISTY1 without FL Function for Higher Order Differential Attack," 13th International (Symposium, Applied Algebra-Algebraic Algorithms and Error-Correcting Codes) 1999, LNCS 1636 (pp 221-231)

EXAMINER	DATE CONSIDERED
----------	-----------------

EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP Section 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.